

Project 1 Report

CS 4371

Group 2:

Peter Cowsar
Sarah Gibbons
Kaleb Jacobsen
Nick Montana
Casey Sledge

February 20, 2018

Introduction

In this project, we learned how to use the security tools, WireShark and NMap. We also learned configuring and setting up networking systems. After familiarizing ourselves with these networking systems we implemented a security policy and created an Access Control Matrix (ACM) to represent the security policy. The group primarily communicated through Slack, an online messaging application, and documented what was done through a collaborative Google Doc. We met primarily on Thursdays after 3:30pm and Fridays from 10am - 3pm. Task 2 was the most significant of the joint efforts by the members, with Sarah, Casey, Nick, and Peter all contributing to the completion of the task. Casey largely handled management of the Cisco firewall, Kaleb and Sarah were largely responsible for implementation and testing of the iptables, Kaleb created the original version of the ACM and was responsible for subsequent edits, and all members contributed to the composition and editing of this final report. Sarah was responsible for the completion of the initial slate-clearing tasks in Task 1.

Task II

Task II was completed by Casey, Sarah, Nick and Peter. Casey and Sarah removed the configuration on Router F via Cisco Control Panel on computer F.1. Nick ran NMap to scan the computers and services on Network F (F.1 and F.2) from server A.F and recorded the results. For task 2.4, Peter executed the experiments specified below to check the default security configuration of the firewall, with all rules removed:

- Ping each computer from each other computer
- Navigate to the web server of each computer from each other computer, internal or external

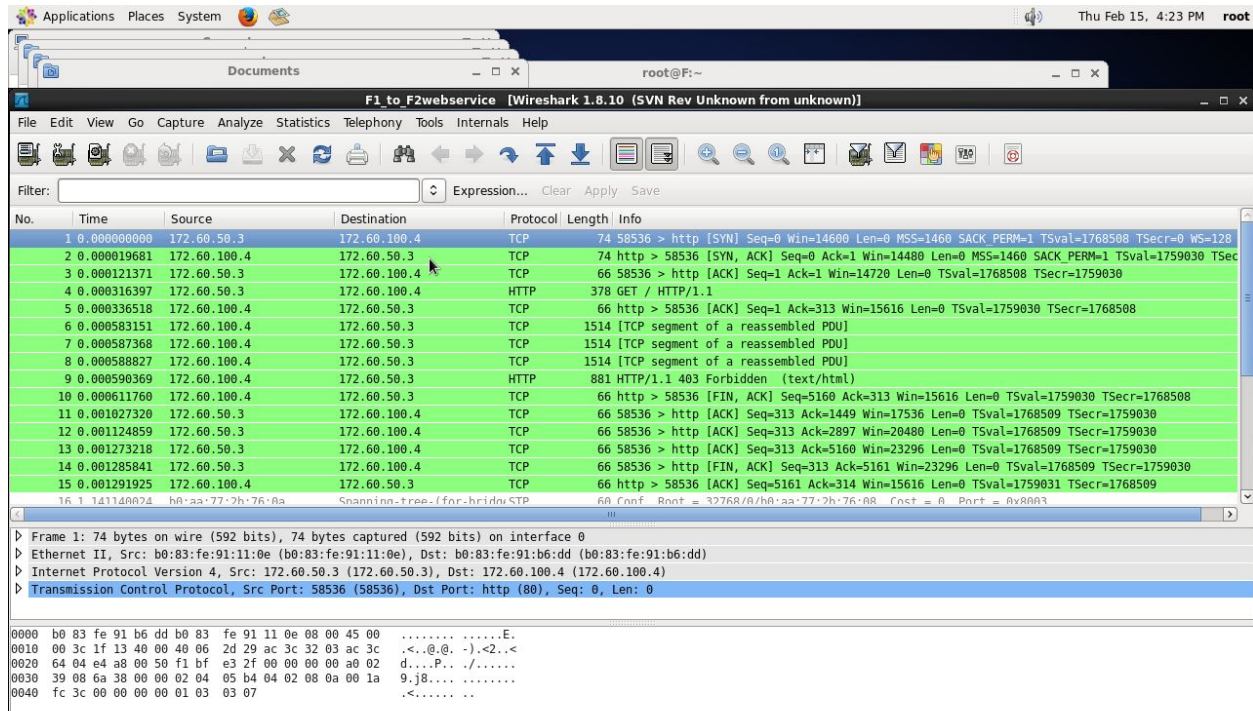
All of the experiments were recorded via Wireshark and the relevant data shown below.

Peter executed the following commands to scan the network F:

```
$ nmap -sV 172.60.50.3
```

```
$ nmap -sV 172.60.100.4
```

Below are the labeled examples from Peter's experiments.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.60.50.3	172.60.100.4	TCP	74	58536 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1768508 TSecr=0 WS=128
2	0.000019681	172.60.100.4	172.60.50.3	TCP	74	http > 58536 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=1759030 TSecr=1768508
3	0.000121371	172.60.50.3	172.60.100.4	TCP	66	58536 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=1768508 TSecr=1759030
4	0.000316397	172.60.50.3	172.60.100.4	HTTP	378	GET / HTTP/1.1
5	0.000336518	172.60.100.4	172.60.50.3	TCP	66	http > 58536 [ACK] Seq=1 Ack=313 Win=15616 Len=0 TSval=1759030 TSecr=1768508
6	0.000583151	172.60.100.4	172.60.50.3	TCP	1514	[TCP segment of a reassembled PDU]
7	0.000587368	172.60.100.4	172.60.50.3	TCP	1514	[TCP segment of a reassembled PDU]
8	0.000588827	172.60.100.4	172.60.50.3	TCP	1514	[TCP segment of a reassembled PDU]
9	0.000590369	172.60.100.4	172.60.50.3	HTTP	881	HTTP/1.1 403 Forbidden (text/html)
10	0.000611760	172.60.100.4	172.60.50.3	TCP	66	http > 58536 [FIN, ACK] Seq=5160 Ack=313 Win=15616 Len=0 TSval=1759030 TSecr=1768508
11	0.001027320	172.60.50.3	172.60.100.4	TCP	66	58536 > http [ACK] Seq=313 Ack=1449 Win=17536 Len=0 TSval=1768509 TSecr=1759030
12	0.001124859	172.60.50.3	172.60.100.4	TCP	66	58536 > http [ACK] Seq=313 Ack=2897 Win=20480 Len=0 TSval=1768509 TSecr=1759030
13	0.001273218	172.60.50.3	172.60.100.4	TCP	66	58536 > http [ACK] Seq=313 Ack=5160 Win=23296 Len=0 TSval=1768509 TSecr=1759030
14	0.001285841	172.60.50.3	172.60.100.4	TCP	66	58536 > http [FIN, ACK] Seq=313 Ack=5161 Win=23296 Len=0 TSval=1768509 TSecr=1759030
15	0.001291925	172.60.100.4	172.60.50.3	TCP	66	http > 58536 [ACK] Seq=5161 Ack=314 Win=15616 Len=0 TSval=1759031 TSecr=1768509
16	1.141140824	b0:aa:77:2b:76:0a	Spanning-tree-for-bridge STP	60 Conf	Root = 32768/8/b0:aa:77:2b:76:08 Cost = 0 Port = 0x8003	

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: b0:83:fe:91:11:0e (b0:83:fe:91:11:0e), Dst: b0:83:fe:91:b6:dd (b0:83:fe:91:b6:dd)
Internet Protocol Version 4, Src: 172.60.50.3 (172.60.50.3), Dst: 172.60.100.4 (172.60.100.4)
Transmission Control Protocol, Src Port: 58536 (58536), Dst Port: http (80), Seq: 0, Len: 0

0000 b0 83 fe 91 b6 dd b0 83 fe 91 11 0e 08 00 45 00E.
0010 00 3c 1f 13 40 00 40 06 2d 29 ac 3c 32 03 ac 3c <...@.-).<2..
0020 64 04 e4 a8 00 50 f1 bf e3 2f 00 00 00 a0 02 d...P.. /.....
0030 39 08 6a 38 00 00 02 04 05 b4 04 02 08 0a 00 1a 9.j8.....
0040 fc 3c 00 00 00 00 01 03 03 07 <.....

F.1 to F.2 Webservice

No.	Time	Source	Destination	Protocol	Length	Info
136	178.039653717	172.60.50.3	172.10.30.15	HTTP	239	GET / HTTP/1.1
140	178.054067094	172.10.30.15	172.60.50.3	HTTP	2345	HTTP/1.1 403 Forbidden (text/html)

F.1 to A.F web Service

41	27.573884716	172.60.100.4	172.10.30.15	HTTP	239	GET / HTTP/1.1
42	27.575096321	172.10.30.15	172.60.100.4	TCP	66	http > 43538 [ACK] Seq=1 Ack=174 Win=15616 Len=0 TSval=2431327488 TSecr=1286242358
43	27.575788734	172.10.30.15	172.60.100.4	TCP	1506	[TCP segment of a reassembled PDU]
44	27.575801255	172.60.100.4	172.10.30.15	TCP	66	43538 > http [ACK] Seq=174 Ack=1441 Win=17536 Len=0 TSval=1286242360 TSecr=2431327489
45	27.575860036	172.10.30.15	172.60.100.4	TCP	1506	[TCP segment of a reassembled PDU]
46	27.575863033	172.60.100.4	172.10.30.15	TCP	66	43538 > http [ACK] Seq=174 Ack=2881 Win=20480 Len=0 TSval=1286242360 TSecr=2431327489
47	27.575995515	172.10.30.15	172.60.100.4	HTTP	2345	HTTP/1.1 403 Forbidden (text/html)

F.2 to A.F Web Service

No.	Time	Source	Destination	Protocol	Length	Info
15	2.043827847	172.60.100.4	172.60.50.3	TCP	74	36890 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460
16	2.043966912	172.60.50.3	172.60.100.4	TCP	60	http > 36890 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

F.2 to F.1 Web Service

(Note: There is no web server on F.1)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	b0:aa:77:2b:76:0a	Spanning-tree-(for-bridg	STP	60	Conf. Root = 32768/0/b0:aa:77:2b:76:08 Cost = 0 Port = 0x8003
2	1.154162909	172.60.100.4	10.32.9.27	DNS	67	Standard query 0xee21 A muug.ca
3	1.154169111	172.60.100.4	10.32.9.27	DNS	67	Standard query 0xb6db AAAA muug.ca
4	1.999861142	b0:aa:77:2b:76:0a	Spanning-tree-(for-bridg	STP	60	Conf. Root = 32768/0/b0:aa:77:2b:76:08 Cost = 0 Port = 0x8003
5	2.952155856	172.10.30.15	172.60.100.4	TCP	74	36012 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1452 SACK_PERM=1 TSval=1146905058 TSecr=0 WS=1
6	2.952171798	172.60.100.4	172.10.30.15	TCP	74	http > 36012 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=1819162 TSecr=1146905058
7	2.953376146	172.10.30.15	172.60.100.4	TCP	66	36012 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=1146905059 TSecr=1819162
8	2.953385387	172.10.30.15	172.60.100.4	HTTP	378	GET / HTTP/1.1
9	2.953399051	172.60.100.4	172.10.30.15	TCP	66	http > 36012 [ACK] Seq=1 Ack=313 Win=15616 Len=0 TSval=1819164 TSecr=1146905059
10	2.953640039	172.60.100.4	172.10.30.15	TCP	1506	[TCP segment of a reassembled PDU]
11	2.953644028	172.60.100.4	172.10.30.15	TCP	1506	[TCP segment of a reassembled PDU]
12	2.953645728	172.60.100.4	172.10.30.15	TCP	1506	[TCP segment of a reassembled PDU]
13	2.953647278	172.60.100.4	172.10.30.15	HTTP	905	HTTP/1.1 403 Forbidden (text/html)
14	2.953669495	172.60.100.4	172.10.30.15	TCP	66	http > 36012 [FIN, ACK] Seq=5160 Ack=313 Win=15616 Len=0 TSval=1819164 TSecr=1146905059
15	2.955012284	172.10.30.15	172.60.100.4	TCP	66	36012 > http [ACK] Seq=313 Ack=1441 Win=17536 Len=0 TSval=1146905061 TSecr=1819164
16	2.955467418	172.10.30.15	172.60.100.4	TCP	66	36012 > http [ACK] Seq=313 Ack=5160 Win=20480 Len=0 TSval=1146905061 TSecr=1819164

A.F to F.2 Web Service

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.10.30.15	172.60.50.3	TCP	74	47070 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460
2	0.001256243	172.60.50.3	172.10.30.15	TCP	60	http > 47070 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

A.F to F.1 Web Service

(Note: There is no web server on F.1)

As shown in these experiments showing the connectivity between the various computers and the other computer's web servers, the default configuration of the router allows all attempts from a computer to any valid web server through. This is, obviously, not optimal from a security perspective.

Below are shown the pings from each computer to each other computer, including external to internal. Sans security policy, this is permitted, but ultimately undesirable.

3	0.467178214	172.60.50.3	172.60.100.4	ICMP	98	Echo (ping) request id=0x8057, seq=5/1280, ttl=64
4	0.467330622	172.60.100.4	172.60.50.3	ICMP	98	Echo (ping) reply id=0x8057, seq=5/1280, ttl=64

F.1 to F.2 Ping

6	4.651158550	172.60.50.3	172.10.30.15	ICMP	98	Echo (ping) request id=0x6e57, seq=1/256, ttl=64
7	4.652417961	172.10.30.15	172.60.50.3	ICMP	98	Echo (ping) reply id=0x6e57, seq=1/256, ttl=62

F.1 to A.f Ping

Filter: icmp		Expression... Clear Apply Save				
No.	Time	Source	Destination	Protocol	Length	Info
18	18.830117923	172.60.100.4	172.60.50.3	ICMP	98	Echo (ping) request id=0x6c52, seq=1/256, ttl=64
19	18.830234064	172.60.50.3	172.60.100.4	ICMP	98	Echo (ping) reply id=0x6c52, seq=1/256, ttl=64
20	19.829484797	172.60.100.4	172.60.50.3	ICMP	98	Echo (ping) request id=0x6c52, seq=2/512, ttl=64
21	19.829605205	172.60.50.3	172.60.100.4	ICMP	98	Echo (ping) reply id=0x6c52, seq=2/512, ttl=64
24	20.829469866	172.60.100.4	172.60.50.3	ICMP	98	Echo (ping) request id=0x6c52, seq=3/768, ttl=64
25	20.829590897	172.60.50.3	172.60.100.4	ICMP	98	Echo (ping) reply id=0x6c52, seq=3/768, ttl=64
30	21.829495418	172.60.100.4	172.60.50.3	ICMP	98	Echo (ping) request id=0x6c52, seq=4/1024, ttl=64
31	21.829609249	172.60.50.3	172.60.100.4	ICMP	98	Echo (ping) reply id=0x6c52, seq=4/1024, ttl=64

F.2 to F.1 Ping

Filter: icmp		Expression... Clear Apply Save				
No.	Time	Source	Destination	Protocol	Length	Info
11	14.148822130	172.60.100.4	172.10.30.15	ICMP	98	Echo (ping) request id=0x4b52, seq=1/256, ttl=64
12	14.150117667	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) reply id=0x4b52, seq=1/256, ttl=62
13	15.150263957	172.60.100.4	172.10.30.15	ICMP	98	Echo (ping) request id=0x4b52, seq=2/512, ttl=64
14	15.151564980	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) replv id=0x4b52, seq=2/512, ttl=62

F.2 to A.F Ping

No.	Time	Source	Destination	Protocol	Length	Info
7	11.115092918	172.10.30.15	172.60.50.3	ICMP	98	Echo (ping) request id=0x3811, seq=1/256, ttl=64
8	11.116389288	172.60.50.3	172.10.30.15	ICMP	98	Echo (ping) reply id=0x3811, seq=1/256, ttl=62

A.F to F.1 Ping

No.	Time	Source	Destination	Protocol	Length	Info
5	3.750678866	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) request id=0x4a11, seq=1/256, ttl=64
6	3.751976186	172.60.100.4	172.10.30.15	ICMP	98	Echo (ping) reply id=0x4a11, seq=1/256, ttl=62

A.F to F.2 Ping

It is evident that the default policy on the Cisco Firewall is overly permissive. It allows all ICMP and HTTP traffic, and even allows vulnerabilities to be discovered via NMap.

Task III

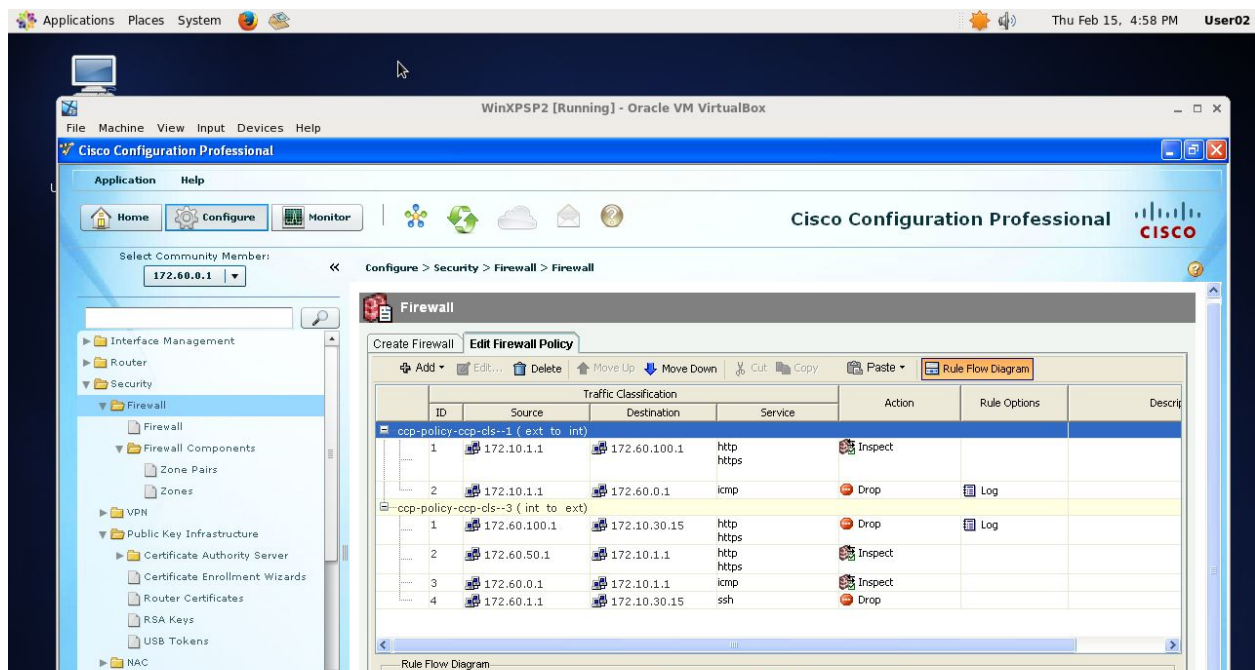
The third task in this project involved the creation and implementation of a new security policy. The policy created specifies that external computers should not be allowed to ping any computers on the internal (F) network, internal computers should be allowed to ping any computer, internal servers should allow internal and external access to their HTTP servers, internal servers should allow only internal access to SSH services, internal servers should not be allowed to access

external web servers, and internal computers should not be allowed to access any external SSH service. The internal workstations should be able to access external HTTP servers. That results in the Access Control Matrix below:

	Internal Workstation (F.1)	Internal Server (F.2)	External Computer (A.F)
F.1	Owns +Ping	+HTTP +Ping +SSH	+HTTP +Ping
F.2	+Ping	Own +HTTP +Ping	+Ping
A.F		HTTP	Own +HTTP +Ping

Matrix of Allowed Actions Between Group F Computers

Not all of the requested policies are possible to implement via the Cisco Firewall, however, as the firewall only checks traffic passing between zones. Traffic between F.1 and F.2, which are on the same interface on the router and thus the same zone, is not able to be secured by the router. Additionally, this traffic never reaches the router as it is directed by the intermediary switch. Because of this, rule of the policy, "Internal servers provide only SSH and web service to internal workstations" cannot be implemented at the router level. Additionally, rule D, "Internal workstations shall not provide any service" can only be partially implemented.



CISCO Firewall Policies Between Internal and External Computers

Of note, while the Firewall Configuration does not reflect it, Casey added an additional rule via Telnet into the router to block all non-matching traffic (access-list 101 deny ip any any).

Because the router-level firewall cannot enforce internal network rules, we need specific policy implementation on each internal computer. For the policy "Internal workstations shall not provide any service" we can simply write an IPtable rule "IPTABLES -A OUTPUT -j DROP" meaning all outgoing signals are blocked from leaving the machine. In the case of the internal server we want to block most traffic but allow specific request. We can achieve this by ordering our IPtables to place specific allowances before a general block.

Our server's IPtable input chain should consist of commands to allow SSH, HTTP and Ping from the internal workstation, as well as HTTP and ping from the external computer, before blocking all other inputs. However, we cannot use a general block for the output chain without limiting the servers ability to respond to request. Instead, we can use a pattern argument to allow all traffic with the ESTABLISHED state to go out from the machine. In practice, this means that only the allowed input

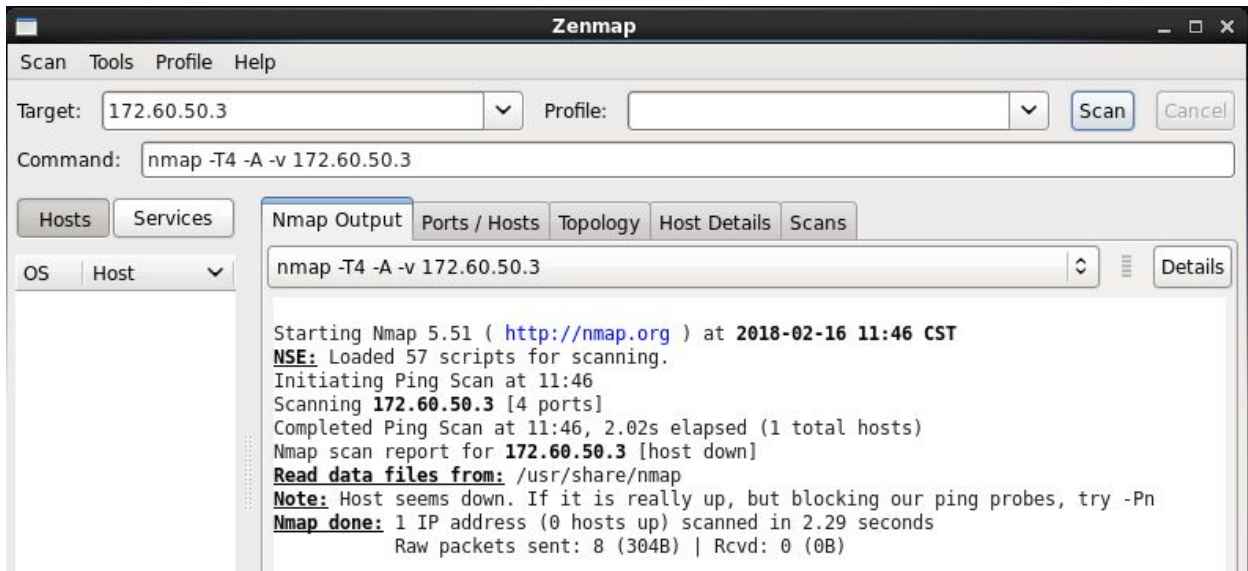
services will be able to establish a connection with our server and receive traffic in response.

```
[User02@F ~]$ sudo iptables -A INPUT -s 172.60.50.3 -p tcp --dport 80 -j ACCEPT
[sudo] password for User02:
[User02@F ~]$ sudo iptables -A INPUT -s 172.60.50.3 -p tcp --dport 22 -j ACCEPT
[User02@F ~]$ sudo iptables -A INPUT -s 172.60.50.3 -p icmp --icmp-type 8 ACCEPT
Bad argument 'ACCEPT'
Try `iptables -h' or 'iptables --help' for more information.
[User02@F ~]$ sudo iptables -A INPUT -s 172.60.50.3 -p icmp --icmp-type 8 -j ACCEPT
[User02@F ~]$ sudo iptables -A INPUT -s 172.10.30.15 -p tcp --dport 80 -j ACCEPT
[User02@F ~]$ sudo iptables -A INPUT -s 172.10.30.15 -p icmp --icmp-type 8 -j ACCEPT
[User02@F ~]$ sudo iptables -j DROP
iptables v1.4.7: no command specified
Try `iptables -h' or 'iptables --help' for more information.
[User02@F ~]$ sudo iptables -A INPUT -j DROP
[User02@F ~]$ iptables --policy FORWARD DROP
iptables v1.4.7: can't initialize iptables table 'filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
[User02@F ~]$ sudo iptables --policy FORWARD DROP
[User02@F ~]$ sudo iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
[User02@F ~]$ iptables -A OUTPUT -j DROP
iptables v1.4.7: can't initialize iptables table 'filter': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
[User02@F ~]$ sudo iptables -A OUTPUT -j DROP
[User02@F ~]$ sudo service iptables start
iptables: Applying firewall rules: [ OK ]
[User02@F ~]$
```

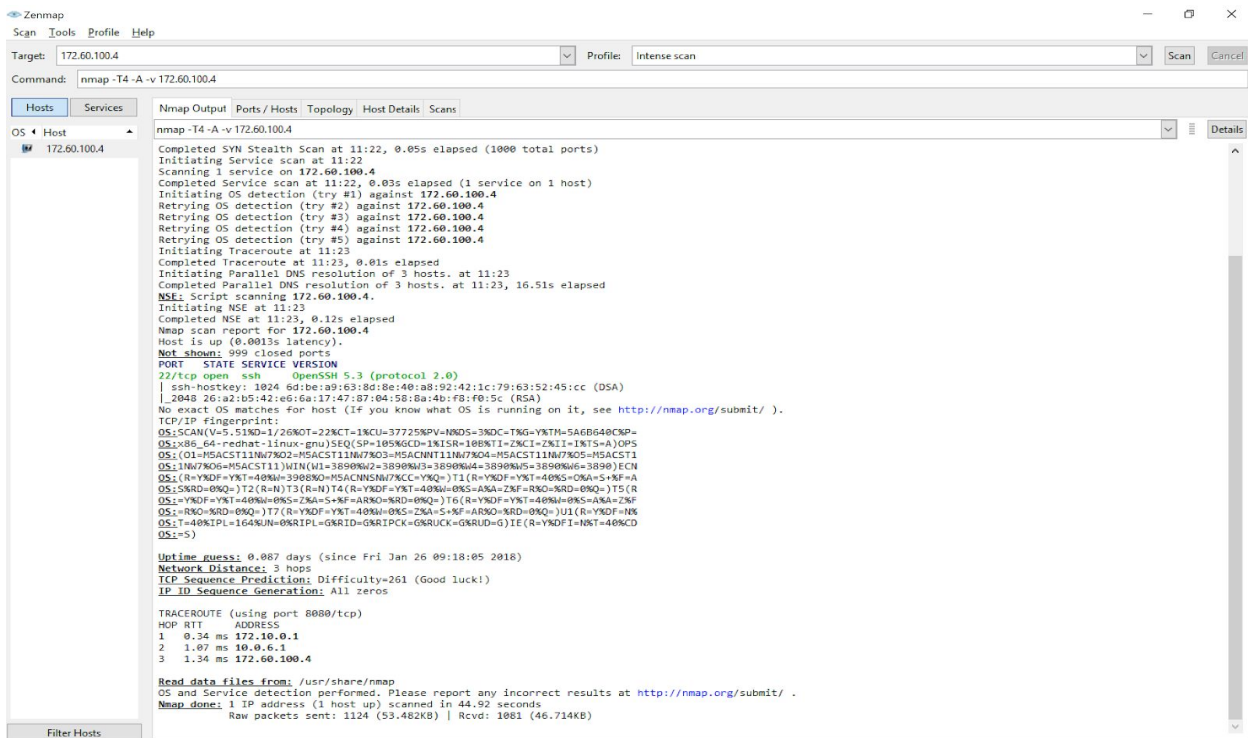
Programming the Internal Server IPtable

Task IV

In order to test the firewall configuration completely, we disabled the iptables firewall on all workstations and servers. The policy was then tested by performing an additional NMap against the internal (F.1, F.2) network. The results of this test are shown below.



A.F to F.1 NMap: Blocked



mapping of computer to computer are shown below. These show that F.1 is able to access the web service on F.2 and A.F, and A.F can access the web server on F.2, but no other combinations are allowed.

No.	Time	Source	Destination	Protocol	Length	Info
18	3.072564716	172.60.50.3	172.60.100.4	HTTP	378	GET / HTTP/1.1
24	3.073802343	172.60.100.4	172.60.50.3	HTTP	2329	HTTP/1.1 403 Forbidden (text/html)
32	3.103907105	172.60.50.3	172.60.100.4	HTTP	359	GET /favicon.ico HTTP/1.1
34	3.104401785	172.60.100.4	172.60.50.3	HTTP	533	HTTP/1.1 404 Not Found (text/html)

F.1 to F.2 Web Server Test (Success)

120	45.439714694	172.60.50.3	172.10.30.15	HTTP	239	GET / HTTP/1.1
126	45.441873929	172.10.30.15	172.60.50.3	HTTP	2345	HTTP/1.1 403 Forbidden (text/html)

F.1 to A.F Web Server Test (Success)

No.	Time	Source	Destination	Protocol	Length	Info
15	2.043827847	172.60.100.4	172.60.50.3	TCP	74	36890 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460
16	2.043966912	172.60.50.3	172.60.100.4	TCP	60	http > 36890 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

F.2 to F.1 Web Server Test (Fail)

Filter: tcp Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.60.100.4	172.10.30.15	TCP	74	43526 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1283897313 TSecr=0 WS=128
3	2.009567560	172.60.100.4	172.10.30.15	TCP	74	43528 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1283899322 TSecr=0 WS=128
5	3.008746254	172.60.100.4	172.10.30.15	TCP	74	[TCP Retransmission] 43528 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1283899322 TSecr=0 WS=128
7	5.008662062	172.60.100.4	172.10.30.15	TCP	74	[TCP Retransmission] 43528 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1283899322 TSecr=0 WS=128

F.2 to A.F Web Server Test (Fail)

Applications Places System						
WiresharkCaptureFirewallPolicyExtToint [Wireshark 1.8.10 (SVN Rev Unknown from unknown)]						
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help						
Filter: Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.60.100.4	172.60.100.4	TCP	74	55146 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=2426270415 TSecr=0 WS=128
2	0.001527978	172.60.100.4	172.10.30.15	TCP	74	http > 55146 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1452 SACK_PERM=1 TSval=1281185284 TSecr=0 WS=128
3	0.001543278	172.10.30.15	172.60.100.4	TCP	66	55146 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=2426270415 TSecr=1281185284
4	4.983582377	172.10.30.15	172.60.100.4	TCP	66	55146 > http [FIN, ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=2426275397 TSecr=1281185284
5	4.984991010	172.60.100.4	172.10.30.15	TCP	66	http > 55146 [FIN, ACK] Seq=1 Ack=2 Win=14592 Len=0 TSval=1281190268 TSecr=2426275397
6	4.985006703	172.10.30.15	172.60.100.4	TCP	66	55146 > http [ACK] Seq=2 Ack=2 Win=14720 Len=0 TSval=2426275398 TSecr=1281190268
7	7.352109548	172.10.30.15	172.60.100.4	TCP	74	53850 > ssh [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=2426277765 TSecr=0 WS=128
8	8.351407033	172.10.30.15	172.60.100.4	TCP	74	[TCP Retransmission] 53850 > ssh [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=2426277765 TSecr=0 WS=128
9	10.351409535	172.10.30.15	172.60.100.4	TCP	74	[TCP Retransmission] 53850 > ssh [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=2426277765 TSecr=0 WS=128
10	14.351404157	172.10.30.15	172.60.100.4	TCP	74	[TCP Retransmission] 53850 > ssh [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=2426277765 TSecr=0 WS=128

A.F to F.1 Web Server Test (Fail)

Filter: http Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
3985	122.935591104	172.10.30.15	172.60.100.4	HTTP	239	GET / HTTP/1.1
3991	122.937692301	172.60.100.4	172.10.30.15	HTTP	2345	HTTP/1.1 403 Forbidden (text/html)

A.F to F.2 Web Server Test (Success)

The security policy stated earlier disallows the external computers to ping the internal computers, but the internal computers should be allowed to ping all computers. The screenshots below show the successful and unsuccessful pings across the network

22	5.596848117	172.60.50.3	172.60.100.4	ICMP	98 Echo (ping) request	id=0xdb55, seq=1/256, ttl=64
23	5.597002977	172.60.100.4	172.60.50.3	ICMP	98 Echo (ping) reply	id=0xdb55, seq=1/256, ttl=64

F.1 to F.2 Ping Test (Successful, shows Reply)

172	68.744288210	172.60.50.3	172.10.30.15	ICMP	98 Echo (ping) request	id=0xa755, seq=1/256, ttl=64
173	68.745749956	172.10.30.15	172.60.50.3	ICMP	98 Echo (ping) reply	id=0xa755, seq=1/256, ttl=62

F.1 to F.2 Ping Test (Successful, shows Reply)

29	16.751070417	172.60.100.4	172.60.50.3	ICMP	98 Echo (ping) request	id=0xff4f, seq=1/256, ttl=64
30	16.751177286	172.60.50.3	172.60.100.4	ICMP	98 Echo (ping) reply	id=0xff4f, seq=1/256, ttl=64

F.1 to F.2 Ping Test (Successful, shows Reply)

Filter: icmp		Expression... Clear Apply Save				
Io.	Time	Source	Destination	Protocol	Length	Info
36	22.073375460	172.60.100.4	172.10.30.15	ICMP	98	Echo (ping) request id=0x1f50, seq=1/256, ttl=64
37	22.074845543	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) reply id=0x1f50, seq=1/256, ttl=62
38	23.074914737	172.60.100.4	172.10.30.15	ICMP	98	Echo (ping) request id=0x1f50, seq=2/512, ttl=64
39	23.076265824	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) reply id=0x1f50, seq=2/512, ttl=62
41	24.076376287	172.60.100.4	172.10.30.15	ICMP	98	Echo (ping) request id=0x1f50, seq=3/768, ttl=64
42	24.077731681	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) reply id=0x1f50, seq=3/768, ttl=62

F.1 to F.2 Ping Test (Successful, shows Reply)

322	8.999921081	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) request id=0xe925, seq=31/7936, ttl=64
356	9.999880305	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) request id=0xe925, seq=32/8192, ttl=64
391	10.999951110	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) request id=0xe925, seq=33/8448, ttl=64
427	11.999899061	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) request id=0xe925, seq=34/8704, ttl=64
461	12.999926084	172.10.30.15	172.60.100.4	ICMP	98	Echo (ping) request id=0xe925, seq=35/8960, ttl=64
790	23.136596202	172.10.30.15	172.60.50.3	ICMP	98	Echo (ping) request id=0xeb25, seq=1/256, ttl=64
822	24.135997005	172.10.30.15	172.60.50.3	ICMP	98	Echo (ping) request id=0xeb25, seq=2/512, ttl=64
856	25.135926204	172.10.30.15	172.60.50.3	ICMP	98	Echo (ping) request id=0xeb25, seq=3/768, ttl=64
891	26.135980784	172.10.30.15	172.60.50.3	ICMP	98	Echo (ping) request id=0xeb25, seq=4/1024, ttl=64
923	27.135926083	172.10.30.15	172.60.50.3	ICMP	98	Echo (ping) request id=0xeb25, seq=5/1280, ttl=64
957	28.135997723	172.10.30.15	172.60.50.3	ICMP	98	Echo (ping) request id=0xeb25, seq=6/1536, ttl=64

A.F to F.1 and F.2 Ping Test (Failure, no Reply received)

Despite our attempts to secure the confidential information stored on computer F.1, including barring the use of flash drives, it is still wholly possible to exfiltrate confidential information from the company's network, given certain conditions. As server F.2 hosts a web server of unknown security measures, it may be possible to POST arbitrary information to the web server via CURL or web server. This information may then be extracted by the same person or by an especially clever

outsider, could retrieve that information by similar method. This issue can only be resolved through clever configuration of deep packet inspection, firewall, iptables, and/or web server configuration to disallow the types and content of connections so proposed. There may exist other vulnerabilities to the network not determined at this time.